Skype Security Assessment

Introduction

Skype is a communication and collaboration application with more than 660 million users. The solution provides free voice and video conferencing between Skype clients and discount long distance calling options to non-Skype phone numbers across the globe. As a result, the service is viewed as a potential cost savings tool for organizations and is worth investigating from a risk and security perspective.

The product is based on the Kazaa peer-to-peer file sharing application and was purchased by Microsoft in 2011. Primary features include:

- Presence information for other Skype users
- Free Skype-to-Skype
  - Voice calls
  - Video calls
  - Instant messaging
- Multi-person video conferencing and group instant messaging
- Screen sharing
- File transfer

Architecture

The peer-to-peer design of Skype requires that users have the ability to connect to each other directly without an intermediary. This traffic is bi-directional with both sides initiating connections. To accommodate this requirement, Skype clients must be made internet available either directly or through a proxy.

Skype recommends that firewalls be opened to allow port 80 and 443 to all Skype clients on internal networks. If that option is not available, a network proxy server must be used that allows any internet client to connect to the Skype user laptops and workstations on the internal network.

Security Risks

The following security risks are associated with the use and implementation of the service:

- Any external, internet Skype user must have the ability to directly access hosts on state networks for the product to function. This turns each workstation into a server that is internet available which could be abused by attackers to host rogue services.
- Skype client vulnerabilities would be able to be leveraged by attackers from the internet due to the architecture of the solution.

- The service uses proprietary tunneling protocols that bypass state security inspection and visibility tools. Without visibility there is greater risk for data loss via hacking or rogue internal users.
- Peer-to-peer file sharing provides a way to both introduce malware and other attack code into the state environment and to easily send sensitive and confidential data to unauthorized external parties.
- IP address and other client information such as BIOS settings are collected by Skype and could be used to map or gain intelligence about state networks and IT infrastructure.
- Recording conversations is also possible with Skype. Users that take part in conversations must be aware of this and avoid discussing sensitive topics if the session is recorded.
- Access and logging information is not maintained on state systems complicating incident response and investigations.

Compliance and Best Practice

According to the OCIO IT Security Standards Skype includes multiple functions that belong to a special class of technologies referred to as "Restricted Services". These include:

1. Peer-to-peer sharing applications
2. Tunneling software design to bypass firewalls and security controls
3. Publically managed chat services and video

As a result, agencies are directed to implement controls to prohibit these functions unless specifically authorized and documented in agency IT security programs. This is a consequence of the significant risks that these restricted services introduce into an environment described above.

CTS is responsible for maintaining the security of state managed networks. To secure the state network, the border firewall is configured to block inbound port 80 and 443 traffic destined for agency networks. Per security best practice, client machines should not host an application made directly accessible to the internet. The Skype peer-to-peer design is not compatible with State network and security architecture from both a policy and infrastructure perspective.

A communication and collaboration solution must be compliant with OCIO IT Security Standards and be compatible with the State's enterprise IT infrastructure. This would include an edge security component that brokers connections between clients on the internal network. The edge component also acts as a trusted bridge for internal to external communication allowing an organization to enforce policy, manage authentication and log the external connections.